

Judgment creditor ZooBuh, Inc., by and through its undersigned counsel, hereby responds to the Objection to Subpoena and Motion to Quash Subpoena to Testify, Produce Documents, Information, or Objects in a Civil Action Issued to Blair Jackson, Esq and Invictus Law, PLLC (the “**Motion to Quash**”), Docket No. 51.

INTRODUCTION

Plaintiff ZooBuh, Inc., a Utah corporation (“**ZooBuh**” or “**Plaintiff**”), sued Defendants Better Broadcasting, LLC, a Utah limited liability company (“**BLLC**”) and IONO Interactive, a Delaware limited liability company (“**IONO**”) in the above-captioned case for violations of the CAN-SPAM Act, 15 U.S.C. §§7701 – 7713. On May 31, 2013, the court entered its Memorandum Decision and Order Granting Default Judgment, reported at 2013 WL 2407669 (the “**Memorandum Decision**”). A copy of the Memorandum Decision is attached hereto as Exhibit A.

Pursuant to the Memorandum Decision, judgment was entered on May 31, 2013 in favor of Plaintiff and against Defendants BLLC and IONO (hereinafter sometimes referred to jointly as the “**Judgment Debtors**”) in the amount of \$1,608,360.00 (the “**Judgment**”), Docket No. 49. No part of the Judgment has been satisfied to date.

In an effort to discover information that might help satisfy the Judgment, Plaintiff issued a subpoena on January 7, 2016 (the “**Subpoena**”) to Blair Jackson and Invictus Law, PLLC (hereinafter sometimes referred to jointly as “**Invictus**”). The Subpoena requires Invictus to produce certain documents, and further requires Blair Jackson to testify at a deposition. A copy of the Subpoena is attached as Exhibit A to the Motion to Quash.

RESPONSE TO FACTUAL ASSERTIONS

1. The Motion to Quash asserts that “the docket shows no discovery attempts of any kind to the Amended Defendants [i.e., BBLLC and IONO].” (Motion to Quash at 3, emphasis in original). Actually, the Subpoena is the Plaintiff’s attempt to find out enough about the Judgment Debtors to seek discovery from them. IONO is the registered agent for, and sole known member of, BBLLC. See corporate printout attached hereto as Exhibit B. IONO is a Delaware limited liability company whose registered agent is another Delaware limited liability company called Dover Delaware Incorporators, LLC (“**Dover**”). When ZooBuh contacted Dover, ZooBuh was informed that Dover’s contact in Utah was Blair Jackson. ZooBuh is not aware of anyone who would be more likely than Blair Jackson and his law firm to have information about BBLLC and IONO.
2. The Motion to Quash asserts that “the docket is silent as to whether notification was made to the Amended Defendants, according to F.R.C.P. Rule 45(a)(4). Such service without the property [sic] notifications is in violation of established rules of civil procedure.” (Motion to Quash at 3) In making this assertion, Invictus is ignoring the effect of F.R.C.P., Rule 5(a)(2), which provides that no service of any papers in a lawsuit is required on a party who is in default for failure to appear. The Judgment Debtors are both in default for failure to appear, and hence are not entitled to notice of the Subpoena. See Memorandum Decision at *1.

ARGUMENT ONE

RULES 1.6 AND 1.9 OF THE UTAH RULES OF PROFESSIONAL CONDUCT DO NOT PROHIBIT JACKSON AND INVICTUS FROM RESPONDING TO THE SUBPOENA

With certain exceptions (one of which is relevant in this case and will be discussed below) Rules 1.6 and 1.9 of the Utah Rules of Professional Conduct prohibit attorneys from voluntarily using or revealing information relating to the representation of a client or former client. The Comments make it clear, however, that both rules apply only to voluntary disclosures, not to situations where information is sought by subpoena.

Comment 3 to Rule 1.6 states as follows:

The principle of client-lawyer confidentiality is given effect by related bodies of law: the attorney-client privilege, the work-product doctrine and the rule of confidentiality established in professional ethics. The attorney-client privilege and work product doctrine apply in judicial and other proceedings in which a lawyer may be called as a witness or otherwise required to produce evidence concerning a client. The rule of client-lawyer confidentiality applies in situations other than those where evidence is sought from the lawyer through compulsion of law.

Utah Rules of Professional Conduct, Rule 1.6, Comment [3] (emphasis added); see *also* Rule 1.9, Comment [7].

In the present case, since Blair Jackson is being called as a witness in a judicial proceeding and Invictus is being asked to produce documents in that same proceeding, the scope and applicability of confidentiality are determined by the attorney-client privilege and work product doctrine, not by Rule 1.6 or 1.9.

Even if Rules 1.6 and 1.9 did apply in the present case, Invictus could be required to provide the information sought in the Subpoena. One of the exceptions to confidentiality is set forth in Rule 1.6(b)(3), which states that the lawyer may reveal information "to prevent, mitigate or rectify substantial injury to the financial interests or property of another that ... has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services." Comment [8] explains that "there will be situations in which the loss suffered by the affected person can be prevented, rectified or mitigated. In such situations, the lawyer may disclose information relating to the representation to the extent necessary to enable the affected persons to ... attempt to recoup their losses."

In the present case, the losses suffered by ZooBuh were due, at least in part, to "false and fraudulent" conduct by IONO and BB, LLC. See Memorandum Decision at *7. Any information Invictus has that would help ZooBuh to discover assets of the Judgment Debtors, or to identify the individuals who control either of the Judgment Debtors, or to show alter ego or a similar remedy, would be helpful as ZooBuh attempts to recoup its losses.

ARGUMENT TWO

THE ATTORNEY-CLIENT PRIVILEGE DOES NOT PROHIBIT JACKSON OR INVICTUS FROM PROVIDING INFORMATION AS REQUIRED BY THE SUBPOENA

The Subpoena requires Invictus to produce documents such as corporate records, tax returns, bank records, and billing records. See Subpoena, attached to the Motion to Quash as Exhibit A. These types of documents are not generally protected by the attorney-client privilege, since the privilege does not extend to “a writing [that] ... involves evidence of objective facts dealing with events, conditions, or circumstances and no expert conclusions or lawyer’s impressions, conclusions, opinions or theories.” *Jackson v. Kennecott Copper Corporation*, 495 P.2d 1254, 1257 (Utah 1972) (emphasis added). Non-privileged writings do not become privileged merely because they are delivered to an attorney by his client. *Id.*

Even documents dealing with the attorney-client relationship are generally not privileged. For example, attorney-client retainer agreements are not privileged. *Gold Standard, Inc. v. American Barrick Resources Corporation*, 801 P.2d 909, 911 (Utah 1990). The reason is that such agreements merely describe “the external trappings of the attorney-client relationship, and are not confidential.” *Id.* For the same reason, documents showing the billing and payment history between attorney and client are not privileged. *In re Walsh*, 623 F.2d 489, 494 (7th Cir. 1980), which was cited with approval in *Gold Standard*, 801 P.2d at 912. Nor are narrative statements in billing

records, unless they reflect litigation strategy. *Freebird, Inc. v. Cimarex Energy Co.*, 264 P.3d 500, 507 (Kan. App. 2011).

In short, most documents held by attorneys in their client files, other than letters and emails between counsel and client, are not generally protected by the attorney-client privilege.

If an attorney believes documents are privileged, the attorney has the burden of establishing that the privilege applies. *McCoo v. Denny's, Inc.*, 192 F.R.D. 675, 680 (D. Kan. 2000). This cannot be done simply by making a blanket assertion of privilege, as *Invictus* has done. Rather, the argument must be “supported by a sufficient description of the nature of the documents, communications or things not produced so as to enable the demanding party to contest the claim.” *Diamond State Insurance Co. v. Rebel Oil Co.*, 157 F.R.D. 691, 697 (D. Nev. 1994); see also F.R.C.P., Rule 45(e)(2)(A).

ARGUMENT THREE

THE WORK PRODUCT DOCTRINE DOES NOT PROTECT THE DOCUMENTS SOUGHT THROUGH THE SUBPOENA

Invictus bears the same burden of proving applicability of the work product doctrine as it does applicability of the attorney-client privilege. The burden was described by Judge Boyce as follows:

[T]he party asserting the work product privilege has the burden of showing the applicability of the doctrine. [cites omitted] The documents must be prepared for the client in anticipation of litigation. [cites omitted] ... A mere allegation of its application is insufficient. [cite omitted]

Lifewise Master Funding v. Telebank, 206 F.R.D. 298, 304 (D. Utah 2002) (emphasis added).

In order to effectively assert the work product doctrine, Invictus must specifically identify the documents it believes are covered by the doctrine, and show that the doctrine covers them.

ARGUMENT FOUR

THE SUBPOENA IS NOT OVERLY BROAD

Invictus argues that the Subpoena is overly broad. (Motion to Quash at 7). Invictus asserts that it has repeatedly asked Plaintiff's counsel to explain why the documents described in the Subpoena are relevant, but has never received a plausible response. *Id.* This is not accurate. In an email dated January 19, 2016, Plaintiff's counsel provided a lengthy explanation of the Subpoena's purpose and objectives. A copy of this email is attached hereto as Exhibit C. Basically, the purpose of the Subpoena is to obtain information about those individuals who may own or control either or both of the Judgment Debtors, including their identity and the nature and extent of their involvement with the Judgment Debtors or companies that may be affiliates of the Judgment Debtors. In addition, the Subpoena seeks information that may lead to income or assets, or that may support alter ego or other equitable claims, for the purpose of satisfying the Judgment.

All of the foregoing purposes are legitimate and appropriate. As noted recently by Judge Waddoups:

The rules governing discovery are to be accorded a broad and liberal treatment. [cite omitted] This is true whether the discovery is part of pretrial or post judgment proceedings. [cite omitted] The purpose of post judgment discovery is to learn information relevant to the existence or transfer of the judgment debtor's assets. [cite omitted] Thus, when supplemental proceedings are an attempt to discover assets by which to satisfy its judgment, plaintiff is entitled to a very thorough examination of the judgment debtor. [cite omitted] This thorough examination includes third parties. Indeed, there is no doubt that third parties can be examined in relation to the financial affairs of a judgment debtor. [cite omitted]

Mountain Dudes, LLC v. Split Rock, Inc., 2013 WL 5435707, *2 (D. Utah 2013) (internal quote marks omitted) (emphasis added).

Invictus complains that it is “nonsensical” to suppose that recent documents could have any relevance to wrongdoing that occurred in 2011. (Motion to Quash at 7). Invictus is missing the point. Plaintiff is not seeking to prove its case against the Judgment Debtors; rather, Plaintiff is trying to satisfy the Judgment, either through assets of the Judgment Debtors or through claims against their insiders and affiliates. For such a purpose, recent documents are likely to be most helpful.

ARGUMENT FIVE

THE SUBPOENA IS NOT UNDULY BURDENSOME

Invictus complains that the Subpoena is unduly burdensome. (Motion to Quash at 8). In order for the Plaintiff and the Court to evaluate this assertion, Invictus needs to disclose the extent of its files (including electronic files), the nature of the documents in the files, the approximate number and length of those documents, and the cost of compliance with the Subpoena. At that point a determination can be made regarding which documents should be produced.

WHEREFORE, Invictus should be ordered to comply with the Subpoena and Blair Jackson should be ordered to appear and testify at a deposition; to the extent that Invictus asserts that the attorney-client or work product privileges protect documents, it should be ordered to identify any and all such documents with particularity and justify the application of any privilege. Plaintiff's reasonable attorney's fees in enforcing the Subpoena should be assessed against Invictus, since Invictus has failed, without adequate excuse, to obey the Subpoena. F.R.C.P., Rule 45(g).

DATED this 11th day of February 2016.

/s/ Chris L. Schmutz
Chris L. Schmutz
Email: chrisschmutz.pc@gmail.com
SCHMUTZ & MOHLMAN, LLC
190 North Main #100
Bountiful, UT 84010

EXHIBIT A

MEMORANDUM DECISION

2013 WL 2407669

Only the Westlaw citation is currently available.
United States District Court,
D. Utah,
Central Division.

ZOOBUH, INC., a Utah Corporation, Plaintiff,
v.

BETTER BROADCASTING, LLC., a Utah limited liability company; **IONO Interactive**, a company doing business in Utah; Does 1–40, Defendants.

No. 2:11cv00516–DN. | May 31, 2013.

Attorneys and Law Firms

Evan A. Schmutz, Jordan K. Cameron, Durham Jones Pinegar PC, Provo, UT, for Plaintiff.

Opinion

MEMORANDUM DECISION AND ORDER GRANTING DEFAULT JUDGMENT

DAVID NUFFER, District Judge.

Introduction

*1 In this action involving unsolicited commercial email communications, commonly referred to as SPAM, plaintiff, ZooBuh, Inc. moved for default judgment, monetary damages, and a permanent injunction against defendants,¹ alleged spammers and alter egos, Better Broadcasting, LLC and IONO Interactive. ZooBuh was represented by Evan A. Schmutz, and Jordan K. Cameron of the law firm of Hill, Johnson & Schmutz, L.C. located in Provo, Utah.

Statement

The Controlling the Assault of Non-Solicited Pornography and Marketing Act located at [15 U.S.C. §§ 7701–7713](#) (“CAN–SPAM Act”) was passed into law in 2003. Somewhat of a misnomer, the CAN–SPAM Act

does not govern non-solicited and pornographic emails only, but rather, in relevant part, prohibits sending any commercial email with header information that is materially false or materially misleading, and requires the provision of certain content in the email bodies.

Plaintiff, ZooBuh, Inc. (“ZooBuh”) was first formed in Utah in 2002 and incorporated in 2007.² ZooBuh is an Internet access service which provides email, chat, and blogging services to approximately 35,000 customers worldwide.³ ZooBuh provides the service through its own equipment.⁴

Between February 18, 2011 and November 7, 2011, ZooBuh received at least 13,453 commercial emails sent and/or initiated by or on behalf of Better Broadcasting and/or Iono, its alter ego,⁵ in violation of various sections of the CAN–SPAM Act.

On November 10, 2011, ZooBuh filed a First Amended Complaint⁶ against the Defendants seeking statutory damages and a permanent injunction. The Defendants failed to appear and answer the Complaint. This Court entered a default certificate against the Defendants on March 7, 2012.⁷ In support of ZooBuh’s claims and request for damages, the Court requested that ZooBuh submit supplemental briefing and evidence on the issues of standing, violations of the CAN–SPAM Act, and damages.⁸

Based on the pleadings and evidence presented to it, the Court finds: 1) that ZooBuh is a bona fide Internet access service who was, and is continually, adversely affected by its receipt of SPAM emails, and therefore qualifies for standing as a private plaintiff under the CAN–SPAM Act; 2) that the emails in question contain violations of [15 U.S.C. § 7704\(a\)\(1\)\(A\)](#), [15 U.S.C. § 7704\(a\)\(1\)\(C\)](#), and [15 U.S.C. § 7704\(a\)\(5\)](#); 3) that the Defendants engaged in practices in violation of [§ 7704\(b\)\(2\)](#); 4) that ZooBuh is awarded damages in the amount of \$1,608,360 and a permanent injunction.

Analysis

I. STANDING

It is well established that “the court *sua sponte*, can raise the issue of standing for the first time at any stage of the litigation.” *New England Health Care Employees Pension Fund v. Woodruff*, 512 F.3d 1283, 1288 (10th Cir.2008) (citing *Rector v. City and County of Denver*, 348 F.3d

935, 942 (10th Cir.2003)). The CAN–SPAM Act dictates that a provider of Internet access service “adversely affected” by a violation of 15 U.S.C. § 7704(a)(1), (b), or (d), or a pattern or practice that violates paragraph (2), (3), (4), or (5) of section 7704(a), may bring a civil action in any district court of the United States with jurisdiction over the defendant to enjoin further violation by the defendant, or to recover damages. 15 U.S.C. § 7706(g)(1). A standing analysis under the CAN–SPAM Act consists of two parts: (1) whether the plaintiff is a *bona fide* Internet access service (see *Gordon v. Virtumundo*, 575 F.3d 1040, 1050 (9th Cir.2009) (citing 150 Cong. Rec. E72–02)); and, (2) whether the plaintiff is adversely affected by SPAM emails (see 15 U.S.C. § 7706(g)(1)). Whether a plaintiff has standing is a necessary question that the Court must answer prior to awarding any damages under the statute.

a. Whether ZooBuh is a Bona Fide Internet Access Service

*2 The CAN–SPAM Act defines Internet access service as “a service that enables users to access content, information, electronic mail, or other services offered over the Internet, and may also include access to proprietary content, information, and other services as part of a package of services offered to consumers. Such term does not include telecommunications services.” 15 U.S.C. § 7702(11); 47 U.S.C. § 231(e)(4). The Ninth Circuit suggested that standing be limited to “bona fide” Internet access services, which is defined in the Congressional Record. “[W]e intend that Internet access service providers provide actual Internet access service to customers.” See *Gordon*, 575 F.3d 1040, 1050 (9th Cir.2009) (citing 150 Cong. Rec. E72–02). The Ninth Circuit also suggested that there exists an ownership and control counterpart to being a bona fide Internet access service. See *Gordon*, 575 F.3d at 1052. *Gordon* held that the plaintiff did not qualify as an Internet access service despite providing email accounts because

Gordon [was] a registrant of a domain name, which he, through Omni, hosts on leased server space. He neither ha[d] physical control over nor access to the hardware, which GoDaddy own[ed], house[d], maintain[ed], and configure[d].... Gordon’s service appears to be limited to using his “Plesk” control panel, which he accesses via an ordinary Internet connection through an ISP, to set up e-mail accounts and log-in

passwords and to execute other administrative tasks. Verizon enables his online access. GoDaddy provides the service that enables ordinary consumers to create e-mail accounts, register domain names, and build personalized web pages. Gordon has simply utilized that service for himself and on behalf of others. *Id.*

Courts have extended the definition of Internet Access Services to “include [] traditional [ISPs], any email provider, and even most website owners.” *MySpace, Inc. v. The Globe.com, Inc.*, No. 06–3391, 2007 WL 1686966, at *3 (C.D.Cal.Feb.27, 2007) see also *Facebook, Inc. v. ConnectU LLC*, 489 F.Supp.2d 1087, 1094 (N.D.Cal.2007).

The Plaintiff, ZooBuh, offers email services, blog hosting, and chat services to its customers.⁹ ZooBuh has customers in all 50 states and in 27 different countries.¹⁰ ZooBuh is widely recognized as a legitimate email provider and has been featured in various publications.¹¹ Unlike the Plaintiff in *Gordon*, ZooBuh owns, maintains and configures all the servers, routers, and switches on its network through which it hosts and provides its internet access services to its customers. Every ZooBuh email account is registered, hosted and serviced through ZooBuh’s own hardware. ZooBuh has sole ownership of all the hardware, complete and uninhibited access to the hardware, and sole physical control over the hardware. ZooBuh also provides each of its customers with their own web-based email portal (which ZooBuh designed, configured, and maintains) through which the ZooBuh customers access their selected web-based services (i.e., email, blogs, chat).¹² Accordingly, ZooBuh is a bona fide Internet access service and satisfies the first part of the standing test under the CAN–SPAM Act.

b. Whether ZooBuh Is Adversely Affected by SPAM

*3 The harm suffered by an Internet access service in order to establish standing under the “adversely affected” part of the CAN–SPAM Act “need not be significant in the sense that it is grave or serious, [but] the harm must be of significance to a *bona fide* IAS [internet access service] provider—something beyond the mere annoyance of spam....” *Gordon*, 575 F.3d at 1053–54. In most cases, evidence of some combination of operational or technical impairments and related financial costs attributable to unwanted commercial e-mail suffice. See *id.* at 1054. Such impairments “include, but are not limited to, network crashes, higher bandwidth utilization,

and increased costs for hardware and software upgrades, network expansion and additional personnel.” *Id.* at 1053 (internal citations omitted). The CAN–SPAM Act does not require that a plaintiff prove that the emails at issue adversely affect the plaintiff, rather, that “[t]he e-mails at issue in a particular case ... contribute to a larger, collective spam problem.” *See Gordon*, 575 P.3d at 1054.

In *Facebook v. Power Ventures, Inc.*, the Northern District of California provided a very helpful analysis of the “adversely affected” requirement for standing. 844 F.Supp.2d 1025 (N.D.Cal.2012). There, the court determined that Facebook’s receipt and analysis of approximately 60,000 messages constituted an adverse effect. *Id.* at 1032. At the time, Facebook’s network consisted of 901 million users and Facebook had over 3,000 employees. *See Facebook “Talking About It.”*¹³ The harm suffered by Facebook with respect to the emails in question was attributable to Facebook’s having to spend time and effort to determine the source of the emails, and taking steps to stop the emails. *Power Ventures* 844 F.Supp.2d at 1031–32. In that case, the court held that Facebook did demonstrate an adverse effect, and that such was especially true because there were a documented 60,000 messages, and “the costs of responding to such a volume of spamming cannot be categorized as ‘negligible.’” *Id.* at 1032.

In its ordinary course of business, ZooBuh utilizes SpamHaus, Razor, Pyzor and Spamassassin as a first line of defense for SPAM received on its system.¹⁴ Despite its efforts to mitigate the harmful effects of SPAM, ZooBuh has experienced hardware crashes, server spikes, bandwidth spikes, kernel crashes, and customer complaints all as the result of a collective spam problem of which the emails in question were a part.¹⁵ If not for its continuous receipt of SPAM email, ZooBuh could successfully service all of its approximately 35,000 customers through four servers.¹⁶ Instead, ZooBuh has had to double its server capacity, at significant expense, in order to successfully service its customers. Even with eight servers, ZooBuh consistently deals with server spikes and crashes, and the servers are constantly pushed to capacity, which significantly decreases the life span of the servers and is expensive in power consumption.¹⁷ Under these facts, ZooBuh satisfies the “adversely affected” requirement as stated by the *Gordon* court.

*4 ZooBuh’s network consists of approximately 35,000 users,¹⁸ ZooBuh has three employees,¹⁹ and there are 13,453 emails at issue.²⁰ Accordingly, the subject emails created a proportionately greater burden for ZooBuh than the 60,000 emails received by Facebook’s 901 million users and over 3,000 employees. Similar to Facebook, for

each email, ZooBuh had to expend man-hours and work to identify the source, examine the transmission information, examine and analyze the header information, take efforts to determine how and why the specific emails were able to circumvent and/or bypass preliminary filtering techniques, and to ultimately attempt to make the emails stop. ZooBuh efforts to deal with the spam cannot be categorized as negligible. *See Power Ventures*, 844 F.Supp.2d at 1032. Under these facts, ZooBuh satisfies the “adversely affected” requirement as stated by the *Facebook* court.

In summary, the harm ZooBuh suffered, and continues to suffer, as the result of its collective SPAM problem is much more significant than the mere annoyance of having to deal with SPAM or the process of dealing with SPAM in the ordinary course of business (i.e., installing a spam filter to flag and discard spam). The harm ZooBuh suffered, and continues to suffer, is manifested in financial expense and burden; lost time; lost profitability; decreases in the life span of ZooBuh’s hardware; server and bandwidth spikes; server crashes; and pre-mature hardware replacements. ZooBuh is adversely affected by a collective spam problem, which includes the emails in question, and that the second part of the standing test is satisfied. Therefore, ZooBuh has standing as defined by the CAN–SPAM Act to assert claims as a private party plaintiff.

II. ANTI–SPAM LAWS

Section 7704(a)(1) of the CAN–SPAM Act dictates that

It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading ... [h]eader information shall be considered materially misleading if it fails to identify accurately a protected computer used to initiate the message because the person initiating the message knowingly uses another protected computer to relay or retransmit the message for purposes of disguising its origin.

15 U.S.C. §§ 7704(a)(1), 7704(a)(1)(C).

Section 7704(a)(1) further dictates that “header information that is technically accurate but includes an originating electronic mail address, domain name, or Internet Protocol address the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations shall be considered materially misleading,” 15 U.S.C. § 7704(a)(1)(A). The conduct prohibited by section 7704(a)(1) is referred to in this order as “Header Violations.”

Section 7704(a)(5) of the CAN–SPAM Act dictates that

*5 It is unlawful for any person to initiate the transmission of any commercial electronic mail message to a protected computer unless the message provides—(i) clear and conspicuous identification that the message is an advertisement or solicitation; (ii) clear and conspicuous notice of the opportunity under paragraph (3) to decline to receive further commercial electronic mail messages from the sender; and (iii) a valid physical postal address of the sender.

The conduct prohibited by section 7704(a)(5) is referred to in this order as “Content Violations.” The CAN–SPAM Act provides statutory damages against parties who engage in a pattern or practice in violation of § 7704(a)(5). 15 U.S.C. § 7706(g)(1).

a. Whether the Emails Contain Header Violations.

There are several decisions arising out of default judgment and summary judgment proceedings wherein the courts awarded damages for Header Violations. In those cases, the various courts determined that Header Violations existed where: the emails failed to identify that they came from the defendant, *see Tagged, Inc. v. Does 1 through 10*, No. C 09–01713 WHA, 2010 WL 370331 (N.D. Cal. Jan 25, 2010); the emails did not accurately identify any party, *see Facebook v. Wallace*, No. C 09–798 JF (RS), 2009 WL 3617789 (N.D.Cal. Oct. 29, 2009); and, the emails contained inaccurate sender names, *see Power Ventures*, 844 F.Supp.2d at 1034–35. Though these decisions are helpful, they do not provide much analysis. Accordingly, it is helpful to look outside of CAN–SPAM decisions for direction on the interpretation

of the statute.

California Business and Professions Code § 17529.5(a)(2) is substantially similar to § 7704(a)(1) of CAN–SPAM in that it prohibits commercial email which “contains or is accompanied by falsified, misrepresented, or forged header information.” Cal. B & P Code § 17529.5(a)(2). Though the language is similar to the CAN–SPAM Act, the California code has been defined as prohibitive of “deceptive” header information only, thereby creating a more onerous burden on a plaintiff than the “materially misleading” standard of the CAN–SPAM Act and thereby avoiding pre-emption by the CAN–SPAM Act. *See Hypertouch v. Valueclick, Inc.*, 192 Cal.App. 4th 805, 825–830 (2011); *Asis Internet Services v. Subscriberbase Inc.*, No. 09–03503 SC, 2010 WL 1267763 (N.D.Cal. Apr. 1, 2010).

In consideration of the California Code’s more onerous burden, the recent California appellate decision in *Balsam v. Trancos* is persuasive as to what constitutes a Header Violation under CAN–SPAM. 138 Cal. Rptr. 3d 108. (Cal.Ct.App.2012). In *Trancos*, the plaintiff sued an email marketer, similar to Defendants in this case, for sending eight commercial email advertisements on behalf of companies that hired the defendant. *Id.* at 112. Before sending the emails, the email marketer privately registered the domains it used to send the emails with a proxy service. *Id.* at 112–13. The proxy service, in turn, displayed the proxy service’s contact information on the domain name registration records instead of the defendant’s contact information. *Id.* A recipient seeking to determine who sent the emails could not determine the sender because the domains were cloaked and a WHOIS look-up would reveal the proxy service’s contact information and not that of the defendant. *Id.* at 118–23.

*6 The appellate court applied CAN–SPAM’s definition of header information and, noting CAN–SPAM’s parallel provision to B & P Code § 17529.5(a)(2), the Court agreed that where the domain names in the emails did not represent a real company and could not be readily traced back to the sender, through available public databases such as WHOIS, such constituted falsification or misrepresentation for purposes of the statute. *Id.* at 122–23. As to privately registered domain names, the Court held “where, as in this case, the commercial e-mailer intentionally uses privately registered domain names in its headers that neither disclose the true sender’s identity on their face nor permit the recipient to readily identify the sender ... such header information is deceptive and does constitute a falsification or misrepresentation of the sender’s identity,” thereby meeting the more strict standard of the California Code.

Id. at 118.

Because the California anti-spam statute has not been preempted, prohibits deception, and imposes a more onerous burden on a plaintiff than does the CAN-SPAM Act, the *Trancos* analysis reasonably extends to the CAN-SPAM Act. Accordingly, where an email contains a generic “from” name and is sent from a privacy-protected domain name, such that the recipient cannot identify the sender from the “from” name or the publicly available WHOIS information, such is “materially misleading” and is a violation of 15 U.S.C. § 7704(a)(1)(C).

In this case 13,333 of the emails contain a generic or nonsensical “from” line that does not identify any real business or individual. Examples of the “from” lines include: “Accounting Degree,” “Add a Sunroom,” “Adult Education,” “Air Conditioner,” “Airline Tickets,” “Ink Cartridges,” and “Ultrasound Technician.”²¹ Additionally, each of the 13,333 emails originated from a sender domain that was privacy-protected.²² Therefore, when a recipient of the email sought to identify the emailer through the publicly available WHOIS database, the WHOIS database record displayed the proxy service’s contact information on the domain name registration records instead of the emailer’s contact information, thereby preventing the recipient from identifying the emailer.²³ Each of these 13,333 emails violates 15 U.S.C. § 7704(a)(1).

Header Violations under the CAN-SPAM Act are not limited to false or misleading header information. Under 15 U.S.C. § 7704(a)(1)(A), even header information that is technically accurate violates the CAN-SPAM Act when the email “includes an originating electronic mail address, domain name, or Internet Protocol address the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations.” 15 U.S.C. § 7704(a)(1)(A).

When a party registers a domain name with an ICANN compliant domain registrar, that registrant enters into a registration agreement with the domain registrar. In most, but not all cases, the domain registration agreement and the accompanying Terms and Conditions (collectively “Registration Documents”) prohibit the use of the registered domain to send unsolicited commercial email or engage in other SPAM practices.²⁴ Accordingly, in order to obtain the domains from the registrar, the registrant represents that it does not intend to use, and will not use, the domains for any purpose prohibited by the Registration Documents. If, as is the case here, the registrant does intend to use the domains for prohibited

purposes, the registrant obtained the domains under a false pretense, and the sending of any email in violation of the Registration Documents violates 15 U.S.C. § 7704(a)(1)(A) on a per email basis.

*7 In this case 13,452 of the emails originated from sender domain names registered with eNom, Inc. and one email originated from a sender domain registered with Moniker Online Services, LLC.²⁵ Each of these registrars requires the party registering the domain to accept its Registration Documents. The Registration Documents of each registrar contain a provision whereby the registrant indicates that they will not use the domain name for purposes of sending unlawful commercial email or SPAM. Accordingly, in order to obtain the domain names used to send the emails in question, the Defendants represented to the domain registrars that the domain names would not be used for SPAM purposes. However, the domain names were intended to be used, and were used, for SPAM purposes. Consequently, the Defendants obtained the sender domains, from which they sent 13,452 emails, under false and fraudulent pretenses in violation of § 7704(a)(1)(A).

b. Whether the Emails Contain Content Violations.

The CAN-SPAM Act requires that any commercial electronic mail message provide (i) clear and conspicuous identification that the message is an advertisement or solicitation; (ii) clear and conspicuous notice of the opportunity to decline to receive further commercial electronic mail messages from the sender; and (iii) a valid physical postal address of the sender. 15 U.S.C. § 7704(a)(5) (collectively “Required Content”).

A determination of whether an email contains a Content Violation turns on the interpretation of the term “clear and conspicuous.” In a commercial communication through an electronic medium “clear and conspicuous” is defined as follows: the “disclosure must be unavoidable ... [and] [a]ny visual message shall be of a size and shade, with a degree of contrast to the background against which it appears, and shall appear on the screen for a duration and in a location sufficiently noticeable for an ordinary consumer to read and comprehend it.” *F.T.C. v. Affiliate Strategies, Inc.*, No. 5:09-CV-04104-JAR-KGS, 2011 WL 3300097, *2 (D.Kan.Aug.1, 2011).

The question presented to the Court in this case is whether Required Content provided in the emails through a remotely hosted image is clearly and conspicuously displayed. This Court determines that it is not.

The body of an email message can be drafted as text only,

HTML, or both by using the MIME protocol.²⁶ Text emails are “plain text,” which means there is no formatting, such as fonts, sizes, and colors. Every email client, even one with the most strict security settings, would likely be capable of reading text emails.²⁷ HTML allows a message to specify font families, sizes, colors, and to have italic, underline or bold letters. Email clients that are configured to read HTML will also read and display text, as HTML-capable email clients are capable of reading and displaying plain text. In contrast, email clients that are only capable of reading text, or email clients that are only configured to read text, will not read and display HTML.²⁸

*8 MIME is an Internet standard that extends the format of email to support message bodies with multiple parts. MIME is specified in six linked RFC memoranda: RFC 2045, RFC 2046, RFC 2047, RFC 4288, RFC 4289 and RFC 2049.2.²⁹ Because MIME extends the format of email to support message bodies with multiple parts, MIME allows email to be drafted in a manner that the email can be read in more than one format. For example, using the MIME protocol, an email can be drafted to have a text part, a HTML part, or both. MIME also allows the emailer to include images as part of the message. There are three main types of images that can be included within an email: “Attached,” “Inline,” and “Remote.”³⁰ At issue in this case are Remote images. Remote images are not part of the email body, but rather a link to a web server that could be anywhere on the Internet and controlled by any unknown third party.³¹

The United States Department of Homeland Security through the United States Computer Emergency Readiness Team (“US–CERT”) is charged with providing response support and defense against cyber-attacks for the Federal Civil Executive Branch and with information sharing and collaboration with state and local government, industry and international partners. US–CERT interacts with federal agencies, industry, the research community, state and local governments, and others to disseminate reasoned and actionable cyber security information to the public. US–CERT repeatedly warns against downloading remotely-hosted images in email.³² In the National Cyber Alert System, Cyber Security Tip ST04–007, US–CERT advised as follows:

Disable the automatic downloading of graphics in HTML mail—Many spammers send HTML mail with a linked graphic file that is then used to track who opens the mail message—when your mail client downloads the graphic from their web server, they know you’ve opened the message. Disabling HTML mail entirely and viewing messages in plain text also

prevents this problem.

National Cyber Alert System, Cyber Security Tip ST04–007, 2.³³

In the document entitled *Recognizing and Avoiding Email Scams*, US–Cert again warns “[t]here are a number of ways you can configure your email client to make you less susceptible to email scams. For instance, configuring your email program to view email as ‘text only’ will help protect you from scams that misuse HTML in email.” *Recognizing and Avoiding Email Scams*, 8.³⁴

Industry also warns of rendering HTML in email messages. In the document entitled *Technical and Policy Requirements for Sending Email to AOL*, AOL warns emailers that they will not support many of the features of HTML.³⁵ AOL also states that “[o]ne reason [the client does not support all features of HTML] is because of the security hazards involved with sending HTML e-mails. These e-mails can expose the unwary user to hostile viruses or other intrusive programs.... The common theme here is end-user security. Malicious e-mailers can bury a wide variety of harmful actions within the HTML e-mail, including programs that activate upon download.” *Technical and Policy Requirements for Sending Email*, 2–3.³⁶

*9 In addition to the security threats inherent in remotely hosted images and the industry standards which typically prevent the display of remotely hosted images in email messages, remotely hosted images are not permanent. If the remotely hosted image no longer exists on the hosting server for any reason, then the image cannot be downloaded to the email client and can never be viewed by the recipient. Remotely hosted images typically do not have a very long shelf-life which means there is a small window of time where the image is viewable by the recipient.³⁷

Given the strong concerns and recommendations against the downloading of remotely hosted images in emails, the industry standards that prevent the automatic download of Remote images in email, and the non-permanent nature of Remote images, the content of remotely hosted images in email communications is not unavoidable and is not likely to appear on the recipient’s screen for a duration and in a location sufficiently noticeable for an ordinary consumer to read and comprehend it. See *F.T.C. v. Affiliate Strategies, Inc.*, 2011 WL 3300097, at*2. This opinion does not address what would constitute a “clear and conspicuous” provision of the Required Content, it merely addresses what is not. It is the opinion of the Court that there are many ways that an emailer could provide the Required Content in a “clear and conspicuous” fashion that would not include the use of Remote images.

In this case none of the Required Content appeared to be provided in the emails in any way. Nevertheless, if the Required Content was provided, it was through remotely hosted images, which images would be blocked by the majority, if not all, email clients, which images would only exist for a short time on a third party server, and which images would not likely be viewed by a recipient. In fact, at the time the emails were received and reviewed by the Plaintiff, none of the Remote images were viewable.³⁸ Accordingly, none of the emails in question provided clearly and conspicuously displayed Required Content and every email violates 15 U.S.C. § 7704(a)(5). Because all of the email in question violates 15 U.S.C. § 7704(a)(5), there is a pattern or practice by the Defendants of violating 15 U.S.C. § 7704(a)(5) and statutory damages are appropriate.

III. DAMAGES

Under the CAN-SPAM Act, a plaintiff may elect to recover monetary damages in an amount equal to the greater of actual losses or statutory damages. 15 U.S.C. § 7706(g)(1)(B). It is well established that “[a] plaintiff may elect statutory damages regardless of the adequacy of the evidence offered as to his actual damages and the amount of the defendant’s profits ... and if statutory damages are elected, the court has wide discretion in determining the amount of statutory damages to be awarded, constrained only by the specified maxima and minima.” *Facebook v. Wallace*, 2009 WL 3617789 at *2 (citing *Columbia Pictures Television, Inc. v. Krypton Broad. of Birmingham, Inc.*, 259 F.3d 1186, 1194 (9th Cir.2001)) (internal quotations omitted).

*10 In this case, ZooBuh elected to recover statutory damages pursuant to 15 U.S.C. § 7706(g)(3)(A) which are calculated by multiplying the number of violations by up to \$100 in the case of Header Violations and up to \$25 in the case of Content Violations. 15 U.S.C. § 7706(g)(3)(A).

In *Wallace*, the court awarded the plaintiff \$710,737,650 in damages. 2009 WL 3617789 at *2. The damage award was calculated by multiplying the number of emails by “\$50.00 per violation of the CAN-SPAM Act.” *Id.* In determining to award \$50.00 per violation, the court looked at various factors. Specifically, the court stated that “[t]he record demonstrates that Wallace willfully violated the statutes in question with blatant disregard for the rights of Facebook and the thousands of Facebook users whose accounts were compromised by his conduct.” *Id.* Wallace’s conduct included violating a temporary restraining order and preliminary injunction. *Id.* Though

the defendant’s actions were severe, the court did not believe that the actions merited an award in excess of seven billion dollars. *Id.* Accordingly, instead of awarding the full \$100 per violation and treble damages, the court scaled back its award to \$50 per violation.

In *Tagged*, the court awarded the plaintiff \$151,975 for 6,079 emails sent by the defendant. 2010 WL 370331, *12. There, the court awarded \$25 per email because the defendant sent only 6,079 emails compared to the greater number of spam messages sent in other cases which had given larger damages awards. *See id.* at 11.

In *Asis Internet Services v. Rausch*, the Court awarded the plaintiff \$865,340 for various violations of 15 U.S.C. § 7704(a)(1) (which carries up to a \$100 penalty) and 15 U.S.C. § 7704(a)(2) (which carries up to a \$25 penalty). 2010 WL 1838752, *7 (N.D.Cal. May 3, 2010). Specifically, the court awarded \$25 per violation of 15 U.S.C. § 7704(a)(1) and \$10 per violation of 15 U.S.C. § 7704(a)(2). The court compared the case to *Wallace* and stated that “[t]his case involves far fewer emails than in [*Wallace*].” *Id.* at *7. Further, the defendant “did not willfully violate an injunction” as was the case in *Wallace*. *Id.* After pronouncing the base award, the court considered the evidence that the defendant had also engaged in dictionary attacks and automated scripting in violation of 15 U.S.C. § 7704(b). *See id.* at *8–9. Based on that fact, the court awarded treble damages as allowed by the statute for a total damage award of \$2,596,020. *Id.* at *9.

The instant case is most similar to *Asis*. Here, there are 13,453 commercial emails in question, each containing one or more violations of the CAN-SPAM Act. Specifically, there are 13,333 emails that violate 15 U.S.C. § 7704(a)(1)(C) (which carries an up to \$100 penalty), 13,453 emails that violate 15 U.S.C. § 7704(a)(1)(A) (which carries an up to \$100 penalty), and 13,453 emails that violate 15 U.S.C. § 7704(a)(5) (which carries up to a \$25 penalty). The emails also contain significant evidence of other spamming practices, which illustrate the willful nature of the violations. Such practices include, but are not limited to, the registration of many .info domain names, image tracking, Bayes Poisoning, scripting, etc.³⁹ Accordingly, this Court applies the *Asis* standard and awards \$25 per violation of 15 U.S.C. § 7704(a)(1)(C) and § 7704(a)(1)(A), and \$10 per violation of 15 U.S.C. § 7704(a)(5) for a total base damage award of \$804,180.

*11 Under the CAN-SPAM Act, the Court can award aggravated damages where the defendant “use[d] scripts or other automated means to register for multiple

electronic mail accounts or online user accounts from which to transmit to a protected computer, or enable another person to transmit to a protected computer, a commercial electronic mail message.” 15 U.S.C. § 7704(b)(2); 15 U.S.C. § 7706(g)(3)(C). Under these circumstances “[t]he court may increase a damage award to an amount equal to not more than three times the amount otherwise available.” 15 U.S.C. § 7706(g)(3)(C).

In this case, there is significant evidence that the Defendants used an automated process through which to create the sender email addresses from which to send the emails in question. Specifically, the sender email addresses, when viewed alphabetically, demonstrate a pattern of words selected in an ascending alphabetical order. Additionally, some of the words cross domain names, indicating that the same script generated the domains by using a dictionary file.⁴⁰ Such practices violate 15 U.S.C. § 7704(b) and entitle a plaintiff to treble damages. 15 U.S.C. § 7704(b)(2); 15 U.S.C. § 7706(g)(3)(C); *Asis*, 2010 WL 1838752 at *9. Accordingly, this Court exercises its discretion to double the statutory damage award and applies the *Asis* standard for a total damage amount of \$1,608,360..

Under the CAN–SPAM Act, the Court can enter an injunction to enjoin further violations by the Defendants. *See* 15 U.S.C. § 7706(g)(1)(A). ZooBuh has substantially prevailed in this matter and has demonstrated the existence of violations of the CAN–SPAM Act in the emails in question. Accordingly, an injunction is entered against the Defendants in this case. The Defendants shall no longer send any commercial email to any ZooBuh customer.

ORDER

ZooBuh’s motions for default judgment⁴¹ and for an order regarding standing and damages⁴² are GRANTED. Defendants are ordered to pay ZooBuh damages in the amount of \$1,608,360. In addition, Defendants are enjoined from further violations of the CAN–SPAM Act.

Footnotes

- ¹ Motion and Memorandum for Entry of Default Judgement, docket no. 28, filed March 1, 2012; Motion to Enter an Order Re Standing and Damages, docket no. 40, filed June 1, 2012.
- ² Declaration of F. Alan Fullmer (Fullmer Declaration) ¶¶ 2, 5, docket no. 43, filed June 1, 2012.
- ³ *Id.* ¶¶ 4, 8.
- ⁴ *Id.* ¶¶ 12–16.
- ⁵ *Id.* ¶ 45.
- ⁶ Docket no. 20, filed November 10, 2011.
- ⁷ Entry of Default, docket no. 29, filed March 7, 2012.
- ⁸ Motion to Enter an Order and Memorandum Re Standing and Damages, docket no. 40, filed June 1, 2012; Memorandum in Support of Motion to Enter Order and Memorandum Re Standing and Damages, docket no. 41, filed June 1, 2012.
- ⁹ Fullmer Declaration ¶ 4.
- ¹⁰ *Id.* ¶ 7.
- ¹¹ *Id.* ¶ 6.

- 12 *Id.* ¶¶ 12–16.
- 13 https://www.facebook.com/pages/Talking-About-It/213156018796346?hc_location=timeline (last visited May 31, 2013).
- 14 *Id.* ¶ 17.
- 15 *Id.* ¶¶ 31–38.
- 16 *Id.* ¶ 25..
- 17 *Id.* ¶¶ 29–30.
- 18 *Id.* ¶ 8.
- 19 *Id.* ¶ 11.
- 20 *Id.* ¶ 45.
- 21 See list attached as Exhibit C to Fullmer Declaration.
- 22 Declaration of Bryceson Ringwood (Ringwood Declaration) ¶ 9, docket no. 42, filed June 1, 2012.
- 23 *See id.* ¶¶ 8–9.
- 24 See eNom Registration Agreement and Abuse Policy, attached as Exhibit E. to Fullmer Declaration; Moniker Registration Agreement, attached as Exhibit F. to Fullmer Declaration.
- 25 Ringwood Declaration ¶ 10.
- 26 Letter of Opinion of F. Alan Fullmer (Fullmer Opinion) ¶ 22, docket no. 38, filed May 31, 2012. For an explanation of these terms, see Fullmer Opinion ¶¶ 1–5.
- 27 *Id.* ¶¶ 23–24.
- 28 *Id.* ¶¶ 26, 28–29.
- 29 *Id.* ¶ 30. The RFC protocols together define email specifications for all Internet users. The Internet Engineering Task Force (“IETF”) codifies standardizing decisions which are then published in Request for Comments (“RFC”). Many RFCs are the standards on which the Internet is formed. By way of example, the Internet Email RFC standards include: RFC 2049, which defines a message representation protocol specifying considerable detail about US–ASCII message headers, and leaves the message content, or message body, as flat US–ASCII text. This set of documents, collectively called the MIME, redefines the format of messages to allow for: (1) textual message bodies in character sets other than US–ASCII; (2) an extensible set of different formats for non-textual message bodies; (3) multi-part message bodies, and (4) textual header information in character sets other than US–ASCII. (Fullmer Opinion at 5, footnote 2.
- 30 *Id.* ¶¶ 31–32.
- 31 *Id.* ¶¶ 35.

32 *Id.* ¶¶ 44–46.

33 *Id.* ¶ 47.. This document is attached to the Fullmer Opinion as Exhibit C.

34 Fullmer Opinion ¶ 49. This document is attached to the Fullmer Opinion as Exhibit D.

35 Fullmer Opinion ¶ 50. This document is attached to the Fullmer Opinion as Exhibit E.

36 Fullmer Opinion ¶ 51.

37 *Id.* ¶¶ 36–37.

38 *Id.* ¶¶ 61–65, 67–70.

39 *Id.* ¶ 66.

40 *Id.* ¶ 66.

41 Docket no. 28, filed March 1, 2012.

42 Docket no. 40, filed June 1, 2012.

EXHIBIT B

CORPORATE PRINTOUT FOR
BETTER BROADCASTING LLC

BETTER BROADCASTING LLC

Entity Number: 7785011-0160

Company Type: LLC - Domestic

Address: 363 N University Avenue STE 110 Provo, UT 84601

State of Origin:

Registered Agent: Iono Interactive

Registered Agent Address:

363 N University Avenue Ste 110

Provo, UT 84601

[View Management Team](#)

Status: [Expired](#)

Status: Expired  as of 12/27/2011

Status Description: Failure to File Renewal

Employment Verification: Not Registered with Verify Utah

[History](#)

[View Filed Documents](#)

Registration Date: 09/17/2010

Last Renewed: N/A

[Additional Information](#)

NAICS Code: 5511 **NAICS Title:** 5511-Management of Companies and Enterpr

[<< Back to Search Results](#)

Search by:

Business Name:

Registered Principals

Name	Type	City	Status
BETTER BROADCASTING LLC	Limited Liability Company	Provo	Expired
Position	Name	Address	
Member	Iono Interactive	363 N University Ave Ste 110	Provo UT 84601
Registered Agent	Iono Interactive	363 N University Avenue Ste 110	Provo UT 84601
If you believe there may be more principals, click here to View Filed Documents			

Search by: [Search Hints](#)

Business Name:

EXHIBIT C

E-MAIL FROM PLAINTIFF'S COUNSEL
DATED JANUARY 19, 2016

Mr. Knowlton: I have reviewed your letter dated January 15, 2016. You have quoted extensively from Rule 1.6 of the Utah Rules of Professional Conduct, but that rule does not apply to this situation. Comment 3 to Rule 1.6 makes clear that an attorney's response to a subpoena is governed by rules relating to the attorney-client privilege and/or attorney work product doctrine, not by the Rules of Professional Conduct. When responding to a subpoena, the governing rule is set forth in UCA section 78B-1-137(2). Under that rule, the identity of the client is not privileged, nor are the terms and conditions of the attorney's employment, the purpose for which the attorney has been retained, or matters relating to fees and payments. *Gold Standard, Inc. v. American Barrick Resources Corporation*, 801 P.2d 909, 911-912 (Utah 1990), and cases cited therein.

Even if Rule 1.6 applied to this case (which it does not), Rule 1.6(b)(3) would require you to provide the requested information. My client, ZooBuh, Inc., has suffered substantial injury to its financial interests as the result of fraudulent activity by Better Broadcasting, LLC ("BB, LLC") and IONO Interactive ("IONO"). Judgment has been entered against both entities in the amount of \$1,608,360.00 (*see* copy of Judgment attached hereto). The Judgment resulted at least in part from fraudulent activity. *See ZooBuh, Inc. v. Better Broadcasting, LLC*, 2013 WL 2407669, *7 (D. Utah 2013).

You have also cited Rule 26, and argued that the subpoena seeks documents that are not relevant and are not proportional to the needs of the case. In response, I would first call to your attention that the subpoena to your firm and Mr. Jackson is a post-judgment collection tool, and in such cases, the limits of relevance are broad. All that need be shown is a nexus between the subpoenaed party and the judgment debtor. *Mountain Dudes, LLC v. Split Rock, Inc.*, 2013 WL 5435707, *2 (D. Utah 2013). In this case, there is a nexus between the judgment debtors, Mr. Jackson, and the other entities and individuals identified in the subpoena. The information we have been able to obtain indicates that IONO is the registered agent and member of BB, LLC. IONO is a Delaware LLC whose registered agent is another Delaware LLC called Dover Delaware Incorporators, LLC. When we contacted Dover Delaware Incorporators we were informed that their contact in Utah is Blair Jackson.

BB, LLC was a Utah company whose principal address was listed as 363 North University Avenue #110 in Provo. The only contact information for BB, LLC on the lease of its office space was a phone number: [\(888\) 419-2464](tel:8884192464). That phone number belongs to MSupport, LLC, whose registered agent was Blair Jackson and whose owner is Ryan Poelman.

The other individual identified in the subpoena, Robert Carney, was apparently the registered owner of many of the domain addresses used by BB, LLC and IONO.

IONO is also listed as the registered agent and member for Common Contact, Expression Media, Factor of 3, and Red Mountain. A common theme for each of these entities is that they rented space which they never occupied and they have no contact information. On Expression Media's lease the only contact information was a phone number [\(888\) 321-1268](tel:8883211268), which also belonged to MSupport.

From the foregoing it is clear that whoever directed the wrongful activity leading to the entry of judgment against BB, LLC and IONO went to considerable lengths to prevent anyone from finding out his or their identity. The best source we have for information regarding the identity of the principals of BB, LLC and IONO is Blair Jackson.

In your correspondence, you have asserted that the subpoena is overly broad, cumbersome and expensive; yet you have also asserted that you do not believe your firm has any of the requested documents. Obviously, the expense and burden depend on the volume of the material. If you do not have any of the requested documents, there is no burden or expense in producing them. On the other hand, if you have large files for each of the entities and individuals identified in the subpoena, the expense and burden could be great. I think it would be worthwhile for us to talk on the phone about the nature and extent of your files and the potential cost of producing documents. I am available most of today. Tomorrow and Thursday I will not be available. Friday I should be available most of the day, especially in the morning. Do you have time available today or Friday?

To help make our phone conversation productive, I can tell you that I am most interested in billing and payment records, corporate records, and correspondence; basically, anything that would identify individuals who own or control the judgment debtors or any of the other entities and that would help me understand the role, level of involvement and contact information for any such individuals, or the relationships of any of the entities with BB, LLC or IONO. The underlying purpose of the subpoena is to locate information leading to assets that could be applied in satisfaction of the judgment or to evidence supporting alter ego, substantive consolidation, or other legal or equitable claims that would allow us to collect on the judgment.

I look forward to hearing back from you.

2 Attachments

Show details